UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,242	06/26/2001	Zheng Qi	BRCMP013C	3440

23363 7590 12/29/2005

CHRISTIE, PARKER & HALE, LLP
PO BOX 7068
PASADENA, CA 91109-7068

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 12/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/892,242	QI ET AL.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/18/2005 has been entered.

Claims 1-37 are pending.

Information Disclosure Statement

Applicant's IDS submitted on 10/18/2005 has been considered.

Response to Amendment

Applicant's amendments have been considered. Please, note new rejections below.

Response to Arguments

Applicant's arguments submitted on 9/9/2005 have been considered, but are moot in view of new grounds of rejections below. Applicant argued that the prior art failed to teach the recited input values are "further based on a select value indicative of whether a current cryptographic operation is to occur during an initial round of a particular series of rounds of cryptographic operations."

The examiner respectfully submits that the above recited limitation that applicant has amended onto the independent claims is extremely broad and even without further search of prior art, the first thing that came to mind about the recited select value is that

it reads on one or more clock signals present in any type of electronic circuit, including the cryptographic circuit disclosed by the prior art of record (Kanda, Callum, and Mano). Clock signals are used to coordinate when certain parts of an electronic circuit is to execute their operation or change state, so in a cryptographic circuit disclosed in the combination invention of Kanda, Callum, and Mano, the signal would be indicative of whether a current cryptographic operation is to occur during an initial round of a particular series of rounds of cryptographic operations. Further, it should also be obvious to one of ordinary skill that since clock signals control the timing/state of circuit components in Kanda, Callum, and Mano's combination invention that the first, second, and third input values would be based on the clock signal(s). The examiner has further cited art below showing how in a cryptographic circuit, a clock signal being used to control the state of a cryptographic circuit was known in the art at the time applicant's invention was made.

Claim Objections

Claims 1 and 23 are objected to because of the following informalities: In the 6th to last line of both claims, the examiner believes that the comma between "value" and "the first" should instead be a semicolon. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 5-12, 14-19, 22-25, 27, 28, 30-34, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al (US 6,769,063) in view of Callum (US 6,320,964) and further in view of Mano ("Digital Design, Second Edition") and Bianco et al (US 5,365,588).

Claims 1 and 23:

Kanda discloses a cryptographic engine as per claim 1 for performing cryptographic operations on a data block (col 1, lines 8-15). Kanda also discloses an integrated circuit layout associated with a cryptography engine as per claim 23 for performing cryptographic operations on a data block, the integrated circuit layout providing information for configuring the cryptography engine (col 1, lines 8-15). Kanda further discloses the cryptographic engine and the integrated circuit layout comprising:

1. A key scheduler configured to provide keys for cryptographic operation (col 7, lines 11-25).
2. Expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a portion of the data block (col 15, lines 8-20 and Figure 8A-8D).
3. Permutation logic configured to alter a second bit sequence corresponding to the portion of the data block (col 1, lines 31-46)

Kanda does not explicitly disclose:

1. Expansion logic coupled to the multiplexer circuitry.
2. Permutation logic coupled to the expansion logic.

However, Callum discloses:

1. Expansion logic coupled to the multiplexer circuitry (Figure 3, items 330 and 319).
2. Permutation logic coupled to the expansion logic (Figure 3, items 319 and 320).

One of ordinary skill in the art at the time the applicant's invention was made would have been motivated to employ Callum's teachings with Kanda because as Callum discloses, his teachings would allow a cryptography engine to better handle instruction-intensive bit permutation and thereby achieve greater cryptography speed (Callum's abstract).

Kanda and Callum both do not explicitly disclose a plurality of logic devices simulating an XOR operation for combining a key provided by the key scheduler with the expanded first bit sequence, the plurality of logic devices including a multiplexer receiving first and second input values and an OR logic combining an output value of the multiplexer with a third input, the first, second, and third input values being determined based on the key provided by the key scheduler and further based on a select value indicative of whether a current cryptographic operation is to occur during an initial round of a particular series of rounds of cryptographic operations.

However, the examiner submits that the above limitation is obvious to the combination invention of Kanda and Callum. The examiner will use the teachings of Mano and Bianco to explain. Kanda is concerned with block ciphering and as such, to encipher/encrypt a block of data, the block is XORed with a subkey, which is provided by a key scheduler (col 7, lines 11-24 and col 10, lines 21-35). Callum also is concerned with block ciphering (col 6, lines 27-30), but more particularly to increasing the speed of the cryptographic engine used for the block ciphering and uses a selector/multiplexer to accomplish this goal (col 1, lines 23-30). In both inventions though, to encrypt/decrypt the data, the data must be XORed with a subkey provided by the key scheduler. Fig 7 of Kanda shows that the subkeys, i.e. the first, second, and third input values, are combined with the expanded first bit sequence. Mano shows on page 144 that the XOR function can be simulated via the use of OR gate(s). Thus it is obvious that the XOR operation in Kanda and Callum's inventions can be simulated via the use of OR gates. To retain the speed advantage from Callum's teachings of a cryptographic accelerator, the output from the multiplexer used by Callum to select the subkey used for the encryption/decryption must be an input to at least one of the OR gates used to simulate the XOR function. One of ordinary skill would be motivated to use OR gates to simulate an XOR function because gate substitution is common practice in the art when certain gates are not readily available and because using certain gates to simulate another gate's function might be needed to achieve a certain timing for a particular part of the circuit. Bianco's teachings are also directed towards cryptography and cryptographic circuits (Fig 1 and col 3, lines 8-10 and 23-24). Bianco

teaches that in cryptographic circuits data transfers and state changes of cryptographic circuits are done according to clock cycles/signals (Fig 4, lines 4-49). Thus the limitation of the first, second, and third input values are further based on a select value indicative of whether a current cryptographic operation is to occur during an initial round of a particular series of rounds of cryptographic operations is obvious from Bianco's teachings. It would have been obvious to one of ordinary skill to further base the first, second, and third input values on a select value, i.e. clock signal, indicative of whether a current cryptographic operation is to occur during an initial round of a particular series of rounds of cryptographic operations at the time applicant's invention was made. One of ordinary skill would have been motivated to do so because electronic circuits, i.e. cryptographic engines, are normally driven by a clock signal.

In light of the above, it would have been obvious to one of ordinary skill in the art to have modified Kanda's invention according to the limitations recited in claims 1 and 23. One of ordinary skill would have been motivated to do so for the reasons given above.

Claims 2 and 24:

Kanda further discloses the cryptographic engine, further comprising an Sbox configuration to alter a third bit sequence having a third size corresponding to the portion of the data block by compacting the third size of the third bit sequence and altering the third bit sequence using Sbox logic (col 3, lines 31-52; col 10, last paragraph; and col 11, 1st paragraph).

Claims 3 and 25:

Kanda further discloses the cryptography engine, wherein the cryptography engine is a DES engine (col 14, lines 15-28).

Claim 5:

Kanda further discloses the cryptography engine, wherein the first bit sequence is less than 32 bits (col 2, lines 1-21).

Claims 6 and 27:

Kanda further discloses the cryptography engine, wherein the first bit sequence is four bits (col 17, lines 9-28).

Claim 7:

Kanda further discloses the cryptography engine, wherein an expanded first bit sequence is less than 48 bits (Figure 10).

Claims 8 and 28:

Kanda further discloses the cryptography engine, wherein an expanded first bit sequence is less than six bits (col 17, lines 9-28).

Claim 9:

Kanda further discloses the cryptography engine, wherein a third bit sequence is less than 48 bits (col 2, lines 22-39).

Claim 10:

Kanda further discloses the cryptography engine, wherein a third bit sequence is six bits (col 2, lines 22-39).

Claim 11:

Kanda further discloses the cryptography engine, wherein the second bit sequence is less than 32 bits (col 2, lines 1-21 and col 10, lines 22-35).

Claim 12:

Kanda further discloses the cryptography engine, wherein the second bit sequence is four bits (col 10, lines 22-35 and col 15, lines 20-53).

Claim 14:

Kanda further discloses the cryptography engine, wherein the key scheduler comprises a plurality of stages (col 1, lines 18-67).

Claims 15 and 30:

Kanda further discloses the cryptography engine, wherein the key scheduler comprises a determination stage (col 15, lines 21-33).

Claims 16 and 31:

Callum further discloses the cryptography engine, wherein the key scheduler comprises a shift stage (col 4, lines 46-67 and col 5, lines 1-5).

Claims 17 and 32:

Kanda further discloses the cryptography engine, wherein the key scheduler comprises a propagation stage (col 2, lines 1-21).

Claims 18 and 33:

Kanda further discloses the cryptography engine, wherein the key scheduler comprises a consumption stage (col 3, lines 30-51).

Claims 19 and 34:

Callum further discloses the cryptography engine, wherein a first shift amount for a first key is identified in the determination stage using a first round counter value (col 4, lines 46-55 and Figure 5).

Claims 22 and 37:

Callum further teaches the cryptography engine, wherein the expansion logic and the permutation logic are associated with DES operations (col 3, lines 32-47 and Fig 3, items 319 and 320).

Claims 4, 13, 20-21, 26, 29, and 35-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al (U.S. 6,769,063) in view of Callum (U.S. 6,320,964), Mano ("Digital Design, Second Edition"), and Bianco et al (US 5,365,588) and further in view of Windirsch (U.S. 6,760,439).

Claims 4 and 26:

Kanda does not explicitly teach a multiplexer circuitry receiving initial data or feedback data from a previous round of cryptographic processing, the multiplexer circuitry including two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on a second level. However, Windirsch teaches a multiplexer circuitry receiving initial data or feedback data from a previous round of cryptographic processing (Fig 1). Note signal R is feedback data from a previous round of cryptographic processing and is fed into multiplexers 9, 23, and 25. Windirsch also

teaches the multiplexer circuitry including two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on a second level (Fig 1, items 13, 25, 29, and 33).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill to further modify Kanda's invention according to the limitations recited in claims 4 and 26 using Windirsch's teachings because Windirsch teachings would allow for a single device that can be operated in different ISO-10116 standard modes (col 1, lines 35-67 and col 2, first paragraph) and allow for simultaneous processing of a number of data streams (col 2, lines 112-16). The examiner further notes that it would have been obvious to one of ordinary skill to have two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on the second level because it would allow for increased performance of DES or triple DES engine as the performance of the computer improved in using 2-to-1 multiplexers. The speed up in clock cycle improves the performance of DES.

Claims 13 and 29:

Kanda does not teach wherein the key scheduler performs pipelined key scheduling logic. However, Windirsch teaches pipelining being used in an encryption/decryption device (col 2, lines 12-35). One of ordinary skill would be motivated to incorporate Windirsch's teachings of pipelining into the combination system of Kanda and Callum as it would allow for simultaneous processing of a number of data streams as disclosed by Windirsch (col 2, lines 12-16).

Claims 20 and 35:

Kanda does not teach a two-level multiplexer receiving initial data or feedback data from a previous round of cryptographic processing. However, Windirsch teaches a two-level multiplexer receiving initial data or feedback data from a previous round of cryptographic processing (col 1, lines 35-47; col 4, lines 51-60; and Fig 1).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to have further modified Kanda's invention according to the limitations recited in claims 20 and 35 in light of Windirsch's teachings. One of ordinary skill would have been motivated to incorporate Windirsch's teachings into the combination system of Kanda and Callum for the same reasons given in claims 4 and 26.

Claims 21 and 36:

Callum teaches the cryptography engine, wherein the multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to the output stage of the multiplexer (col 3, lines 48-61; col 1, lines 39-46; and Fig 3).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ponnoreay Pich
Examiner
Art Unit 2135

Primary Examiner
Art Unit 2135

PP